FEDERAL AVIATION ADMINISTRATION—WASHINGTON, DC

CHANGE 2

EFFECTIVE: DECEMBER 28, 1995
APRIL 21, 1997

Part 129—Operations: Foreign Air Carriers and Foreign Operators of U.S.-Registered Aircraft Engaged in Common Carriage

This change incorporates two amendments:

Amendment 129–25, Revision of Authority Citations, adopted December 20 and effective December 28, 1995, updates the authority citations listed in the Code of Federal Regulations to reference current law. No substantive change is introduced to Part 129 by this amendment.

Amendment 129–26, Sensitive Security Information, adopted March 13 and effective April 21, 1997, amends Part 129 by adding § 129.31.

Bold brackets enclose the newly added material. The amendment number and effective date appear in bold brackets at the end of each section.

Page Control Chart

Remove Pages	Dated	Insert Pages	Dated
P–87	Ch. 1	P–87 through P–99	Ch. 2
Pages 1 through 7	Ch. 1	Pages 1 through 7	Ch. 2

Suggest filing this transmittal at the beginning of the FAR. It will provide a method for determining that all changes have been received as listed in the current edition of AC 00–44, Status of Federal Aviation Regulations, and a check for determining if the FAR contains the proper pages.

Act. However, this amendment is considered significant under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979).

The Amendment

In consideration of the foregoing, the Federal Aviation Administration amends parts 121, 129, and 135 of the Federal Aviation Regulations (14 CFR part 121, 14 CFR part 129, and 14 CFR part 135) effective December 29, 1994.

The authority citation for part 129 continues to read as follows:

Authority: 49 U.S.C. app. 1346, 1354(a), 1356, 1357, 1421, 1502, and 1511; 49 U.S.C. 106(g) (Revised Pub. L. 97–449, January 12, 1983).

Amendment 129–25

Revision of Authority Citations

Adopted: December 20, 1995 **Effective: December 28, 1995**

(Published in 60 FR 67254, December 28, 1995)

SUMMARY: This rule adopts new authority citations for Chapter I of Title 14 of the Code of Federal Regulations (CFR). In 1994, the Federal Aviation Act of 1958 and several other statutes conferring authority upon the Federal Aviation Administration were recodified into positive law. This document updates the authority citations listed in the Code of Federal Regulations to reference the current law.

DATES: This final rule is effective December 28, 1995. Comments on this final rule must be received by March 1, 1996.

FOR FURTHER INFORMATION CONTACT: Karen Petronis, Office of the Chief Counsel, Regulations Division (AGC–210), Federal Aviation Administration, 800 Independence Ave., SW., Washington, DC 20591; telephone (202) 267–3073.

SUPPLEMENTARY INFORMATION: In July 1994, the Federal Aviation Act of 1958 and numerous other pieces of legislation affecting transportation in general were recodified. The statutory material became ''positive law'' and was recodified at 49 U.S.C. 1101 *et seq.*

The Federal Aviation Administration is amending the authority citations for its regulations in Chapter I of 14 CFR to reflect the recodification of its statutory authority. No substantive change was intended to any statutory authority by the recodification, and no substantive change is introduced to any regulation by this change.

Although this action is in the form of a final rule and was not preceded by notice and an opportunity for public comment, comments are invited on this action. Interested persons are invited to comment by submitting such written data, views, or arguments as they may desire by March 1, 1996. Comments should identify the rules docket number (Docket No. 28417) and be submitted to the address specified under the caption ''FOR FURTHER INFORMATION CONTACT.''

Because of the editorial nature of this change, it has been determined that prior notice is unnecessary under the Administrative Procedure Act. It has also been determined that this final rule is not a ''significant regulatory action'' under Executive Order 12866, nor is it a significant action under DOT regulatory policies and procedures (44 FR 11034, February 26, 1979). Further, the editorial nature of this change has no known or anticipated economic impact; accordingly, no regulatory analysis has been prepared.

Amendment 129–26

Sensitive Security Information

Adopted: March 13, 1997 **Effective: April 21, 1997**

(Published in 62 FR 13736, March 21, 1997)

SUMMARY: This final rule strengthens the existing rules protecting sensitive security information from unauthorized disclosure. Part 191 is expanded to apply to air carriers, airport operators, indirect air carriers, foreign air carriers, and individuals, and specifies in more detail what sensitive security information they must protect. Part 191 continues to describe what information is protected from disclosure by the FAA, and describes in more detail that information. This final rule also changes parts 107, 108, 109, and 129 to correspond with changes it makes to part 191. This action is necessary to counter the increased sophistication of those who pose a threat to civil aviation and their ability to develop techniques to subvert current security measures. The intended effect of this action is to prevent undue disclosure of information that could compromise public safety if it falls into the wrong hands, while being mindful of the public's legitimate right to know and interest in aviation information.

FOR FURTHER INFORMATION CONTACT: Eugene Cunningham, Office of Civil Aviation Security Division (ACP–100), Office of Civil Aviation Security Policy and Planning, Federal Aviation Administration, 800 Independence Avenue, SW., Washington, DC 20591; telephone (202) 267–8701.

SUPPLEMENTARY INFORMATION:

Background

The Security Regulatory Scheme

The FAA is required to prescribe rules, as needed, to protect persons and property on aircraft against acts of criminal violence and aircraft piracy, and to prescribe rules for screening passengers and property for dangerous weapons, explosives, and destructive substances. See, 49 U.S.C. 44901 through 44904. To carry out the provisions of the statute, the FAA has adopted rules requiring airport operators, air carriers, indirect air carriers, and foreign air carriers to carry out various duties for civil aviation security. Title 14, Code of Federal Regulations, part 107 (14 CFR part 107) applies to certain airport operators. Part 108 (14 CFR part 108) governs certain air carriers.

Part 109 (14 CFR part 109) applies to indirect air carriers such as freight forwarders, who engage indirectly in air transportation of property. Part 129 (14 CFR part 129) applies to the operation of foreign air carriers within the United States.

Parts 107, 108, 109, and 129 contain general requirements for promoting civil aviation security. Each airport operator, air carrier, indirect air carrier, and foreign air carrier covered by these parts also has a security program that is approved or accepted by the Administrator, containing information that specifies how airport operators and air carriers perform their regulatory and statutory responsibilities. These security programs are available only to persons with the need-to-know, as described more fully below.

Each air carrier's security program is a comprehensive document that details the full range of security procedures and countermeasures that air carriers are required to perform under 14 CFR § 108.5. This program includes procedures for: (1) Screening of passengers, carry-on baggage, checked baggage, and cargo; (2) using screening devices (such as X-ray systems and metal detectors); (3) controlling access to aircraft and air carrier facilities; (4) reporting and responding to bomb threats, hijackings, and weapons discovered during screening; (5) reporting and protecting bomb threat information; (6) identifying special

program and the system for maintaining records.

The indirect air carrier security program covers security procedures for cargo that is accepted for transport on air carrier aircraft. In general, indirect air carriers are required to carry out security procedures for handling cargo that will be carried on air carrier aircraft.

Foreign air carriers' security programs provide security procedures for foreign air carriers while operating to and from the United States, which is a counterpart to the procedures required under part 108.

Security programs of individual companies are based largely on standard security programs and amendments developed by the FAA and industry. As new threats are identified and improved countermeasures developed, the FAA develops standard means to respond to the threats and improve security.

Other sources of information and countermeasures are contained in the Security Directives and Information Circulars, described in § 108.18. These sources address threats to civil aviation security as well as responsive countermeasures to those threats. Additionally, these sources provide sensitive information concerning various security devices, such as metal detectors and X-ray machines.

The Need to Protect Security Information

The notice of proposed rulemaking contained a history of how the threat to civil aviation has increased over the years. The FAA monitors potential threats to civil aviation. Terrorists pose an increasingly sophisticated threat to civil aviation. This has led the FAA to reevaluate the release of security information to the public, particularly in response to requests under the FOIA. This information has been termed sensitive security information (SSI).

It is important to keep details of security measures and FAA evaluations of security out of the public domain where terrorists could read them. If the information identified in this rule were publicly available, it could reveal potential weaknesses in the current security system.

The FAA is mindful of the public's legitimate interest in how the FAA operates and how it regulates the aviation industry, as well as how the industry is carrying out its duties. The FAA has a corresponding responsibility to prevent undue disclosure of information that could compromise public safety if it falls into the wrong hands. The rule has been carefully considered and covers only information that could reasonably be anticipated to be damaging to the security of the traveling public if given to unauthorized persons.

Security programs are absolutely essential mechanisms through which the FAA regulates the air carriers' and airports' detailed obligations with respect to ensuring civil aviation security. Much of the effectiveness of the programs depends on strictly limiting access to such information to those persons who have a need-to-know. Unauthorized disclosure of the specific provisions of the air carrier and airport security programs or other aviation security information would allow potential attackers of civil aviation to devise methods to circumvent or otherwise defeat the security provisions. It would also discount the deterrent effect inherently provided in prohibiting disclosure of security measures that may or may not be in place.

There are sophisticated criminal elements who actively seek information on what seemingly are minor security points, with a view to accumulating a larger picture of the entire security program. Therefore, it is imperative that the entire security program be protected. Similarly, it is critical to protect the information contained in Security Directives and Information Circulars. These documents contain detailed information on threats that the FAA has identified, and the measures to counter those threats. The unauthorized release of that information could compromise those countermeasures. In addition, particular information regarding FAA approved security devices, such as metal detectors, should also be protected to the extent possible.

Part 191 states when the FAA will withhold certain requested information from public disclosure, such as when requested under the Freedom of Information Act (FOIA) (5 U.S.C. 552), in litigation, or in rulemaking. Part 191 currently applies only to the FAA, and does not specify all of the sources of SSI that should be covered.

Civil aviation security information protected under the Federal Aviation Regulations is different from Classified National Security Information governed by Executive Order 12598 and related orders, statutes, and rules. The Executive Order provides for classifying information as Top Secret, Secret, and Confidential, and covers a wide range of information affecting the national security. All persons with access to such information must have an appropriate security clearance, and there may be a criminal penalty for misuse of the information. While there is some ''classified'' civil aviation security information, part 191 is not directed to the handling of classified information. Indeed, part 191 is needed because the SSI is not National Security Information and therefore is not subject to the controls that apply to such information.

This final rule improves the protection of SSI by amending parts 107, 108, 109, 129, and 191 as described more fully later in the document.

Discussion of Comments

The FAA published Notice of Proposed Rulemaking No. 94–32 on December 6, 1994 (59 FR 62956). In response to Notice No. 94–32, 17 comments were received from a total of 18 commenters, 2 commenters having jointly submitted 1 comment.

Five commenters state that the proposed language in proposed § 191.5(a) on the release of SSI is too broad. Of these, two commenters ask the FAA to limit this language by linking the enforcement of SSI unauthorized releases to significant compromises of security or those that result in an actual security incident.

The FAA believes the suggested language would weaken the rule. The FAA should not have to wait to see if the improperly released or compromised information is actually misused before taking action against the person(s) who released it. On the contrary, one purpose of the rule is to have more clear and consistent guidance as to what must be protected. In every case in which the FAA considers what enforcement action to take in response to a violation, however, the FAA considers all factors, including the potential or actual adverse impact on safety or security.

The same two commenters also share the view that the FAA should limit the geographic scope of airport security programs solely to that area where scheduled carriers operate. These commenters argue that this geographic limitation would remove general aviation operations from the Air Operations Area (AOA), reducing the number of individuals with a ''need-to-know'' and thereby reducing the potential for the release of SSI.

The FAA finds that the scope of the airport security program would be more appropriately addressed in part 107. If needed, airport operators may contact their cognizant FAA security office for a re-evaluation of the geographic areas in which security measures are applied.

Six commenters request the addition of language to proposed § 191.5(a) or (d) to make clear that, if an air carrier or airport operator has established a reasonable procedure for the control of sensitive information and has not been negligent in monitoring compliance with this procedure, the air carrier or airport operator would not be held to a standard of strict liability for disclosures made by individuals.

Currently § 108.7(c)(4) requires each air carrier to ''restrict the availability of information contained in the security program to those persons with an operational need-to-know . . .'' Current § 107.3(e) requires in part that each airport operator ''restrict the distribution, disclosure, and availability of information contained in the security program to those persons with an operational need-to-know . . .'' Proposed § 191.5(a) would impose similar duties on airport operators and air carriers, stating that they must ''restrict disclosure of and access to sensitive security information to persons with a need-to-know, . . .'' The

hold a Department of Defense (DOD)-approved SECRET clearance. Nonetheless, the commenters say they do support the premise that individuals should be penalized if they have acted imprudently or knowingly disregarded the instructions of their employers. The commenters state that even with the clearest of instructions regarding the protection of the information, it is unreasonable to expect air carriers to be totally responsible for the actions of a large number of individuals.

As noted earlier in this document, the air carriers' responsibility under the rule will be similar to their responsibilities under the current rule, and air carriers that are in compliance now need not change their procedures. SSI is not Classified National Security Information, and no Secret clearance issued by the Federal government is required to gain access to it. The FAA realizes that certain employees will have access to SSI simply because they must retrieve the information from facsimile machines and the like, although they do not have responsibility to carry out the security program. All such employees, however, are responsible for protecting the information from unauthorized disclosure.

Three commenters ask how agencies or persons, included within the scope of the proposed regulation, should respond to Freedom of Information Act (FOIA) or Open Records Act (ORA) requests for unclassified security information, in the event the proposed regulation is promulgated as written.

The requirement to make records available under the FOIA does not apply to matters that are specifically exempted from disclosure by statute (5 U.S.C. 552(b)(3)). Under 49 U.S.C. 40119, the information described in the rule is exempt by statute from disclosure. When the FAA receives requests under FOIA for SSI, the FAA will deny the information in accordance with § 191.3. As to requests for information under state and local freedom of information acts or open records acts, § 191.5(a) provides that requests for SSI be referred to the Administrator. The FAA works with the airports and air carriers to determine what records or portions of records should remain undisclosed, and what may be released.

Ten commenters state that the proposed regulation restricts, too severely, the disclosure of SSI. Three of these commenters object that the proposed language may prohibit disclosure of security information to a carrier president, outside counsel, consultant, or management personnel who do not personally perform or directly supervise security activities. Five commenters indicate that the carriers may be required to inform parties other than those with a need-to-know of certain security requirements or procedures. Such parties may include travel agents, passengers, contractors, and internal personnel who develop procedures to ensure effective passenger, cargo, and baggage processing for the air carrier.

The FAA believes that the definition of "need-to-know" as proposed would have provided for dissemination of information to travel agents, passengers, contractors, and internal personnel, when such dissemination is necessary to carry out security duties. The FAA agrees, however, that the proposed definition could have been read as more limiting than intended, as to some persons. Various high level officials must be apprised of the information, even though they may not personally carry out the security requirements. Further, persons who represent the air carriers and airport operators, such as attorneys and industry associations, may have a need-to-know, in order to be able to represent their clients. In order to avoid misunderstanding, the FAA is clarifying the definition of need-to-know in § 191.5(b) to read as follows: A person has a need-to-know sensitive security information when the information is necessary to carry out FAA-approved or directed aviation security duties; when the information is necessary to supervise or otherwise manage the individuals carrying out such duties; to advise the airport operator, air carrier, indirect air carrier, or foreign air carrier regarding the specific requirements of any FAA security related requirements; or to represent the airport operator, air carrier, indirect air carrier, or foreign air carrier, or person receiving information under § 191.3(d) in connection with any judicial or administrative proceeding regarding those requirements. For some specific information, the Administrator may specify which persons, or classes of persons, have a need-to-know.

Three commenters indicate that contractors who are bidding on a job inside the security identification display area (SIDA) need to know what the procedures are for ID applications and employment history checks in order to price their bids correctly. One of these commenters states that "each person issued an airport identification badge has a need to know certain details of the Airport Security Program."

In this commenter's opinion, the proposed draft acknowledges that the foreign government has a need-to-know in the case of a foreign air carrier, but not necessarily in connection with the overseas operation of a U.S. air carrier.

The FAA finds that the foreign government would also meet the need-to-know requirement in connection with the overseas operations of a U.S. air carrier. Procedures have already been established through FAA liaison personnel and the State Department to communicate necessary security information.

Two commenters state that many airport operators must supply monthly confiscated weapons reports or incident reports to other official bodies, sometimes for the purpose of prosecution at the local level. Another commenter notes that, local law enforcement or legislative requirements may require disclosure of certain security information to persons otherwise without a ''need-to-know'' as part of normal reporting requirements. This commenter requests coordination among industry and FAA personnel before the FAA designates information as ''sensitive.''

It appears that most confiscated weapons reports would not be SSI, if the airport operator is releasing the report. Section 191.7(h) makes such information SSI only as to release by the FAA. As to the release of other information to law enforcement officials, or in response to other legislative requirements, the airport operator should contact the FAA to discuss specific needs. Some of the information the commenter is concerned about may not be SSI under the rule. As to information that is SSI, the FAA may approve release to specific states and local officials with appropriate safeguards to prevent its dissemination to unauthorized persons.

One commenter indicates that, if sensitive information concerns a specific airport, persons having a need-to-know should include, at a minimum, the designated Airport Security Coordinator(s). This commenter also states that Coordinators should have the authority to disseminate such information themselves on a need-to-know basis among parties at the airport or within the same airport authority.

The FAA agrees with the commenter to the extent that the need-to-know requirements apply.

One commenter states that the proposed disclosure limitations may preclude carriers from seeking assistance form government agencies or other law enforcement authorities when faced with unusual security situations or threats.

It appears that, if the air carrier is seeking assistance to respond to security situations or threats, there is a need-to-know within the meaning of the rule. Of course, the agency or authority should be informed of the nature of the information and the need to not release it to unauthorized persons.

One commenter asks that proposed § 191.5(c) be modified to include whistle-blower protection for the entity that advises the FAA that a breach of security has occurred. This commenter observes that, ''without a safeguard, there will be a tendency for parties . . . not to advise the FAA (that a breach of security has occurred) in the hope that they would not be caught . . . .''

The primary purpose of § 191.5(c) is to permit the FAA to evaluate the release of information and determine whether there is a need to act to mitigate any vulnerability the release might have caused. The fact that a person self-discloses a failure to comply with the rule is given significant weight in determining what, if any, action should be taken as to that person. In the end, the choice of action involves the exercise of prosecutorial discretion, and will be considered in the context of policies involving enforcement in general.

Four commenters ask for modification of proposed § 191.5(d) to specify the FAA's criteria for adequate restriction of access to, or disclosure of, sensitive information; to clarify what changes might be recommended by the FAA to security procedures; and to state the actions that may be included in the phrase ''other enforcement or corrective action,'' including potential criminal prosecution.

As noted previously, the air carriers' and airport operators' responsibilities under the new rule are similar to their responsibilities under the current rules. Procedures that are appropriate under the current rules should be continued, and a similar level of protection should be used for other SSI.

a certificate). In appropriate cases, the FAA may refer a matter to proper authorities for criminal prosecution.

Two commenters request modification of proposed § 191.7 to list, as completely as possible, the specific categories of information which fall within the meaning of the phrase SSI. These commenters state that such a list should include training programs and records of practice exercise as a category.

The entire training program of an air carrier is not normally SSI. However, the program contains SSI, such as specifications of test objects and security devices, and sensitive procedures. Under § 191.7, the portions of the training programs containing SSI must be protected, but the rest is not subject to this rule.

Similarly, training records are not normally considered SSI in themselves, because they normally do not contain SSI. They may simply indicate the dates that the screeners completed their training, for instance. Such records are a general means by which the FAA monitors industry compliance with specific requirements, and therefore would not require protection in accordance with § 191.7. However, there are occasions when information related to "sensitive activities," such as practical exercises, which falls under the purview of § 191.7(d), is included in training records. Under these circumstances, those particular training records would be subject to part 191 controls.

These two commenters also ask whether the airport boundary descriptions found in airport security plans are SSI, whether information that is readily available elsewhere become SSI by being included in an airport security plan, whether partial disclosures of information contained in an airport security plan might violate the proposed regulation, and if so, what the threshold of violation by partial disclosure might be.

Informaiton that is not in the security plan or otherwise listed in § 191.7 is not SSI under this rule. Because the airport boundary descriptions are readily available elsewhere, they can be released in the form that is available elsewhere without violating the new rule.

These commenters also suggest that the FAA reconsider the necessity of designating all threat information as sensitive. According to these commenters, it would be more efficient to draw a distinction between information regarding general trends in terrorist technology and possible responses, which is largely in the public domain and should not be subjected to extensive disclosure protection, and known, specific threats.

It is not clear to which portion of the rule the commenters are objecting. New § 191.7(i) (proposed as § 191.7(h)(1)) makes threat information SSI only as to release by the FAA, which means that the FAA may decline to release the information. That section does not require the airport operator or air carrier to protect the information. Airport operators and air carriers are required to protect threat information that may be a part of security program amendments, Security Directives, and Information Circulars, because they are protected under § 191.7(a) and (b). It should also be noted that general trends in terrorist technology and possible responses often is non-public, and may even be Classified National Security Information.

Two commenters state that the FAA cost/benefit analysis is not correct. Of these, one commenter states that evidence does not exist to support the FAA's portrayal of the terrorist threat to civil aviation, as found in the section of the NPRM titled "The Need To Protect Security Information."

The FAA disagrees with this commenter. The information reflected in the "Need To Protect Security Information" section of the NPRM is based on a complete analysis of the best threat information available.

The other commenter in this group states that, if the proposed regulation is adopted, the air carriers will have to inform their employees of the new regulations and will also have to design a more sophisticated tracking system in order to trace the dissemination of security information. Dollars will have to be spent to secure information in safes, locked rooms, and to purchase shredders and conduct audits. The commenters state that there is the potential cost to the carriers to investigate and respond to FAA allegations of noncompliance, which more often than not results in a civil penalty.

reasonably necessary to adequately protect the public.

The Rule As Adopted

Part 191

Part 191 sets forth the rules that allow the FAA to withhold information from public disclosure. This final rule amends and reorganizes part 191 as follows:

Section 191.1 is expanded to apply not only to the FAA, but also to air carriers, airport operators, indirect air carriers, foreign air carriers, and individuals. As discussed later in this document, parts 107, 108, 109, and 129 still would contain some requirements regarding the protection of information, but part 191 would be the primary rule for withholding information from unauthorized disclosure.

Section 191.1(a) is amended to conform to the current statute. In 1976, the FAA promulgated part 191 to implement the Air Transportation Act of 1974, Public Law 93–366. Section 316(d)(2) of the Federal Aviation Act of 1958, as amended, provided, in part, that the Administrator shall prescribe regulations to "prohibit disclosure of any information obtained or developed in the conduct of research and development activities" if the disclosure meets certain conditions. This section is a major basis for the current rules in part 191 on withholding information from unauthorized disclosure.

In 1990, section 316(d)(2) was amended to provide that the Administrator shall adopt rules to prohibit disclosure of "any information obtained in the conduct of security *or* research and development activities. . . ." Section 9121 of the Aviation Safety and Capacity Expansion Act of 1990 (Pub. L. 101–508) (emphasis added). In 1994 this section was recodified, and now appears at 49 U.S.C. 40119. This final rule amends § 191.1(a), to protect information obtained during the course of specified security activities. This final rule also removes from the title of part 191 reference to the 1974 Act, to avoid any implication that it is the only source of statutory authority for the part.

Section 191.1(b) now defines "record," in part, as "documentary" material. This final rule removes the word "documentary." It addresses all methods of preserving information, including computer records. This would avoid any misunderstanding over whether such records were "documentary."

Part 191 now refers to the "Director of Civil Aviation Security" as the official who makes the determination on behalf of the Administrator to withhold information. Under internal FAA reorganization, the current title of this position is Associate Administrator for Civil Aviation Security, however, 49 U.S.C. 44932 refers to this official as Assistant Administrator for Civil Aviation Security. Therefore, part 191, as adopted, uses the title "Assistant Administrator for Civil Aviation Security." In addition, the Deputy Assistant Administrator for Civil Aviation Security (currently called the Deputy Associate Administrator for Civil Aviation Security) and any individual formally designated to act in the capacity of the Assistant Administrator or the Deputy, now has the authority to make such determinations.

For decisions involving information and records described in § 191.7(a) through (g), and related documents in (l), § 191.1(c) permits delegation below the Assistant Administrator level. The information that is described in § 191.7(a) through (g) is well-defined, and decisions on release or withholding of the information involves relatively objective judgments.

Section 191.7(h), (i), (j), (k), and related documents described in (l), require more subjective judgments. A decision to release or withhold information under these paragraphs requires a careful evaluation of the need to provide the highest level of security to the traveling public by preventing SSI from falling into the wrong hands, balanced by an awareness of the public's strong interest in obtaining information about security in air transportation. These decisions require a careful evaluation of security threats as well as important policies of the agency. Therefore, this rule requires that such decisions be made by high policy-level officials, and not below the Assistant Administrator and Deputy Assistant Administrator level. The Assistant Administrator is responsible for carrying out the agency's civil aviation security program, and reports directly to the Administrator.

or designated representative for the sole purpose of providing the information necessary to prepare a response to the allegations contained in the legal enforcement action document. Such information is not released under the FOIA.

Whenever such documents are provided to an alleged violator or designated representative, the Chief Counsel or designee advises the alleged violator or designated representative that: (a) The documents are provided for the sole purpose of providing the information necessary to respond to the allegations contained in the legal enforcement action document; and (b) SSI contained in the documents provided must be maintained in a confidential manner to prevent compromising civil aviation security.

Section 191.5, as adopted, contains the requirements that apply to persons other than the FAA. Such persons include air carriers, airport operators, indirect air carriers, foreign air carriers, and persons who receive SSI in connection with enforcement actions, and individuals employed by, or contracted by, air carriers, airport operators, indirect air carriers, foreign air carriers, and persons who receive SSI in enforcement actions. This section is intended to be very inclusive.

A difficult aspect of protecting SSI is that a large number of persons must be aware of at least portions of the information in order to carry out their duties including pilots, flight attendants, ticket agents, screeners, baggage handlers, and law enforcement officers. Frequently, some of these people are not direct employees of the air carrier or airport operator, but they do carry out duties for, or on behalf of, the air carrier or airport operator. For example, in many cases, screeners and law enforcement officers are not directly employed by air carriers or airport operators, but do have important security responsibilities to carry out. This section is intended to cover all such persons who have access to SSI. It should be emphasized, however, that airports and air carriers will continue to have the responsibility they now have to protect SSI. If SSI is released to unauthorized persons, depending upon the circumstances, the FAA may hold the airport or air carrier, as well as the individual accountable.

Section 191.5(a) states the general requirement that disclosure of, and access to, SSI shall be restricted to persons with a need-to-know. Section 191.5(b) defines need-to-know as when the information is necessary to carry out FAA-approved or directed aviation security duties; when the information is necessary to supervise or otherwise manage the individuals directly carrying out such duties; to advise the airport operator, air carrier, indirect air carrier, or foreign air carrier regarding the specific requirements of any FAA security related requirements; or to represent the airport operator, air carrier, indirect air carrier, or foreign air carrier, or person receiving information under § 191.3(d) in connection with any judicial or administrative proceeding regarding those requirements.

In most cases, the air carrier or airport operator has the discretion to decide who in its organization has a need to know SSI. There are times, however, when information is so sensitive that extra measures should be taken to protect that information from release to those without a need-to-know. The rule would, therefore, provide that for some specific information the Administrator may make a finding that only specific persons, or classes of persons, have a need-to-know.

Section 191.5(c) requires that, if sensitive security information is released to unauthorized persons, the FAA must be notified. This will permit the FAA to evaluate the risk presented by the release of the information, and to take whatever action may be needed to mitigate that risk.

Section 191.5(d) alerts persons that violations may result in a civil penalty or other action by the FAA. The FAA may take a broad range of enforcement action for violation of the regulations. The FAA anticipates that civil penalty action will be considered for a violation of part 191, as it is for violations of parts 107 and 108. However, the FAA may seek enforcement action deemed appropriate based on individual circumstances of the case. Further, the FAA may take action to mitigate or correct the risk posed by the violation. Such actions may include requiring air carriers or airport operators to change their procedures for protecting security information, or change the security procedures in place that may have been compromised by unauthorized release of the information.

this information available. Air carriers and others would not be expected to protect those details.

Second, the Administrator may release some other SSI to help achieve compliance with the security requirements. In rare circumstances the FAA has released summary information regarding air carriers' failures to fully carry out their security duties, which assisted in bringing them into compliance. In such cases, the FAA must determine whether security will be better served by maintaining the confidentiality of the information, or to release some portions of it to help achieve compliance with the security standards.

The introductory text of § 191.7 also refers to "records containing such information" as being SSI. This would include, for instance, interpretations that contain information on the contents of security programs and other SSI.

Section 191.7(a) retains the current requirements to protect any approved or standard security program for an air carrier, indirect air carrier, airport operator, or foreign air carrier. It also is clarified to protect any security program that relates to United States mail to be transported by air (including that of the United States Postal Service and of the Department of Defense). This rule expands this provision to include any comments, instructions, or implementing guidance pertaining to these security programs. Generally, these materials reveal some or all of the sensitive information and must be protected the same as the security programs themselves.

Section 191.7(b) is revised to include any comments, instructions, or implementing guidance pertaining to Security Directives and Information Circulars.

New § 191.7(c) lists any profile used in any security screening process, including persons, baggage, or cargo. Hijacker and baggage screening profiles were previously addressed in current § 191.3(b)(1) and (2). This rule now makes those profiles general to cover screening persons, because there are systems in place to protect against terrorists and others who might seek to commit criminal violence, not just hijackers. This rule addresses cargo profiles because, like baggage, cargo is a potential tool for criminal violence that the security rules cover.

Section 191.7(d) includes any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto. These plans, when adopted, become part of the security program and are already covered by rules governing security programs; however, they are included in § 191.7 for emphasis.

This rule deletes the provisions currently in current § 191.3(b)(6), pertaining to the technical specifications for devices for protection against, or detection of, cargo theft. Such devices are not directly used to meet the requirements for civil aviation security under the FAA regulations. Any devices that serve a dual function of protecting cargo and security are protected under other provisions in this section.

Section 191.7(e) covers the technical specifications of any device used for the detection of any "deadly or dangerous weapon, explosive, incendiary, or destructive substance." It is essentially the same as the current § 191.3(b)(5) which used the words "explosive or incendiary device or weapon," with the addition of the phrase "destructive substance." That phrase is used in 49 U.S.C. 44902 in reference to searching persons and property to be carried aboard aircraft.

Section 191.7(f) addresses the descriptions of and technical specifications of objects used to test screening equipment and equipment parameters. Knowledge of this test equipment and parameters could lead to a plan to defeat those devices. Accordingly, details of such devices should be protected.

Section 191.7(g) addresses the technical specifications of any security communications equipment and procedures. Knowledge of security communication equipment and procedures could lead to a plan to defeat those devices. Accordingly, details of such devices should be protected.

Section 191.7(h) addresses release of certain information relating to violation of the security rules. Section 191.7(h) applies only to the release of information by the FAA. There is less risk of harm from casual disclosure of this information by individuals. The FAA, however, has information regarding

in the system, to make that information less useful in identifying apparent weaknesses.

Section 191.7(h) as adopted provides generally for withholding any information that the Administrator has determined may reveal a systemic vulnerability of the aviation system or a vulnerability of aviation facilities to attack. This is defined to include certain details of inspections, investigations, and alleged violations and findings of violations of 14 CFR parts 107, 108, or 109, or §§ 129.25, 129.26, or 129.27, and any information that could lead to the disclosure of such details. For events that occurred less than 12 months before the date of the release of the information, the FAA will not release the name of an airport where a violation occurred, the regional identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of the air carrier in connection with specific locations or specific security procedures. The FAA may release summaries of an air carrier's total security violations in a specified time range without identifying specific violations. Summaries may include total enforcement actions, total proposed civil penalty amounts, total assessed civil penalty amounts, number of cases opened, number of cases referred by Civil Aviation Security to FAA counsel for legal enforcement action, and number of cases closed.

For events that occurred 12 months or more before the date of the release of the information, FAA will not release the specific gate or other location on an airport where the event occurred.

In addition, the FAA will not release the identity of the FAA special agent who conducted the investigation or inspection, or security information or data developed during FAA evaluations of the air carriers and airports and the implementation of the security programs, including air carrier and airport inspections and screening points tests or methods for evaluating such tests.

Section 191.7(i) (proposed as § 191.7(h)(1)) covers release by the FAA of information concerning threats against civil aviation. This paragraph specifically applies only to release of information by the FAA. However, threat information may also be contained in Security Directives, Information Circulars, or other documents that air carriers and others must protect under other provision of this section.

Section 191.7(j) further clarifies that the FAA does not release, and others should not release, certain details of security measures not otherwise listed in this section, such as information regarding Federal Air Marshals. Release of such information to unauthorized persons could not only compromise security, it could place Federal Air Marshals in danger.

Secton 191.7(k) includes any other information that the Administrator determines should not be disclosed under the criteria in § 191.3(b). While we have attempted to anticipate all sources of information that should be protected from unauthorized disclosure, additional information may be discovered in the future. This section allows the Administrator to determine whether that additional information should or should not be considered as SSI.

Section 191.7(l) includes any draft, proposed, or recommended changes to SSI or records. The FAA frequently issues proposed revisions for sensitive security documents to air carriers and airport operators and requests comments on the proposals. These proposals contain SSI that also should be protected.

Parts 107, 108, 109 and 129

This rule change also affects those specific sections of parts 107, 108, 109, and 129 which require airport operators, air carriers, indirect air carriers, and foreign air carriers to protect security information and direct requests for such information to the Administrator as required in part 191.

All changes to parts 107, 108, 109, and 129 correspond to, and are redundant with, changes made to part 191 because airport operators, air carriers, and foreign air carriers refer to their specific parts of Title 14 CFR for security requirements. Including a cross-reference to part 191 in parts 107, 108, 109, and 129, alerts airport operators and air carriers to the new requirements, and makes it clear that part 191 is part of their security duties.

Regulatory Evaluation Summary

Benefits and Costs

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866 directs that each Federal agency shall propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 requires agencies to analyze the economic effect of regulatory changes on small entities. Third, the Office of Management and Budget directs agencies to assess the effect of regulatory changes on international trade. In conducting these analyses, the FAA has determined that this rule is not "a significant regulatory action" as defined in the Executive Order and the Department of Transportation Regulatory Policies and Procedures. This rule will not have a significant impact on a substantial number of small entities and will not constitute a barrier to international trade.

A detailed discussion of costs and benefits is contained in the full evaluation in the docket for this Final Rule. The costs and benefits associated with this Final Rule are summarized as follows.

Air carriers and airports have security programs which are intended to protect the public from the threat of aircraft hijacking and other criminal activities affecting air transportation. The FAA proposes to strengthen the rules protecting security-related information from being released to unauthorized persons. The current rules fail to require individuals to protect sensitive security information that is in their control, and specify all sensitive security information that should be protected from public disclosure.

The unauthorized disclosure of any of the information contained in these security programs can have a detrimental effect on the ability to thwart terrorist and other criminal activities. This final rule will amend parts 107, 108, 109, and 129 to restrict the distribution, disclosure, and availability of specific sensitive security information, which will be defined in part 191, to persons with a need-to-know.

Because this fine rule will not be included in the airport or the air carrier security programs, and because there are no specific requirements for safes, locked files, or enhanced security equipment, affected entities will not incur any costs to implement these proposed requirements.

Much of the air carrier and airport security program effectiveness depends on strictly limiting access to sensitive security information to those persons who have a need-to-know. Sophisticated criminal elements are actively seeking ways to obtain information regarding the methods and procedures used by the FAA, air carriers, and airports to guard against terrorist activities. The accumulation of seemingly minor security details can enable the criminal element to piece together a larger picture of the entire security program. Therefore, it is imperative that the entire security program be protected.

The consequences of not protecting such information can be catastrophic. Between 1982 and 1991, terrorist bombings of U.S. air carriers have resulted in 275 deaths and 24 injuries, while hijackings incidents have resulted in 24 deaths and 127 injuries.

Given the absence of cost and the potential benefits of avoided fatalities and injuries, this final rule is cost beneficial.

Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980 (RFA) was enacted by Congress to ensure that small entities are not unnecessarily burdened by government regulations. The RFA requires agencies to review rules that may have a "significant economic impact on a substantial number of small entities." FAA Order 2100.14A, Regulatory Flexibility Criteria and Guidance, establishes threshold costs and small entity size standards for complying with RFA requirements. There is no cost associated with this rule; therefore, it does not have a significant economic impact on a substantial number of small entities.

This rule will not have a substantial direct effect on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 12612, it is determined that this rule does not have sufficient federalism implications to warrant preparation of a Federalism Assessment.

Conclusion

For the reasons discussed above, and based on the findings in the Regulatory Flexibility Determination and the International Trade Impact Statement, the FAA certifies that this regulation will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act. This rule is not considered a ''significant regulatory action'' under Executive Order 12866 and is considered nonsignificant under Order DOT 2100.5, Policies and Procedures for Simplification, Analysis, and Review of Regulations. A regulatory evaluation of the rule, including a Regulatory Flexibility Determination and International Trade Impact Analysis, has been placed in the docket. A copy may be obtained by contacting the person identified under ''FOR FURTHER INFORMATION CONTACT.''

The Amendment

Accordingly, the Federal Aviation Administration amends parts 107, 108, 109, 129, and 191 of Title 14, Code of Federal Regulations (14 CFR parts 107, 108, 109, 129, and 191) effective April 21, 1997.

The authority citation for part 129 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40104–40105, 40113, 40119, 44701–44702, 44712, 44716–44717, 44722, 44901–44904, and 44906.

Part 129—Operations: Foreign Air Carriers and Foreign Operators of US.-Registered Aircraft Engaged in Common Carriage

§ 129.1 Applicability.

(a) Except as provided in paragraph (b) of this section, this part prescribes rules governing the operation within the United States of each foreign air carrier holding a permit issued by the Civil Aeronautics Board or the Department of Transportation under Section 402 of the Federal Aviation Act of 1958 (49 U.S.C. 1372) or other appropriate economic or exemption authority issued by the Civil Aeronautics Board of the Department of Transportation.

(b) Section 129.14 also applies to U.S.-registered aircraft operated in common carriage by a foreign person or foreign air carrier solely outside the United States. For the purpose of this part, a foreign person is any person, not a citizen of the United States, who operates a U.S.-registered aircraft in common carriage solely outside the United States.

Docket No. 24856 (52 FR 20029) 5/28/87; (Amdt. 129–12, Eff. 4/28/82); (Amdt. 129–14, Eff. 8/25/87)

§ 129.11 Operations specifications.

(a) Each foreign air carrier shall conduct its operations within the United States in accordance with operations specifications issued by the Administrator under this part and in accordance with the Standards and Recommended Practices contained in part I (International Commercial Air Transport) of Annex 6 (Operation of Aircraft) to the Convention on International Civil Aviation Organization. Operations specifications shall include:

(1) Airports to be used;

(2) Routes or airways to be flown; and

(3) Such operations rules and practices as are necessary to prevent collisions between foreign aircraft and other aircraft.

(4) Registration markings of each U.S.-registered aircraft.

(b) An application for the issue or amendment of operations specifications must be submitted in duplicate, at least 30 days before beginning operations in the United States, to the Flight Standards District Office in the area where the applicant's principal business office is located or to the Regional Flight Standards Division Manager having jurisdiction over the area to be served by the operations. If a military airport of the United States is to be used as a regular, alternate, refueling, or provisional airport, the applicant must obtain written permission to do so from the Washington Headquarters of the military organization concerned and submit two copies of that written permission with his application. Detailed requirements governing applications for the issue or amendment of operations specifications are contained in appendix A.

(c) No person operating under this part may operate or list on its operations specifications any airplane listed on operations specifications issued under part 125.

(Amdt. 129–14, Eff. 8/25/87); (Amdt. 129–19, Eff. 10/25/89)

§ 129.13 Airworthiness and registration certificates.

(a) No foreign air carrier may operate any aircraft within the United States unless that aircraft carries current registration and airworthiness certificates issued or validated by the country of registry and displays the nationality and registration markings of that country.

(b) No foreign air carrier may operate a foreign aircraft within the United States except in accordance with the limitations on maximum certificated weights prescribed for that aircraft and that operation by the country of manufacture of the aircraft.

§ 129.14 Maintenance program and minimum equipment list requirements for U.S.-registered aircraft.

(a) Each foreign air carrier and each foreign person operating a U.S.-registered aircraft within or outside the United States in common carriage shall ensure that each aircraft is maintained in accordance with a program approved by the Administrator.

(b) No foreign air carrier or foreign person may operate a U.S.-registered aircraft with inoperable

The foreign operator must show, before minimum equipment list approval can be obtained, that the maintenance procedures used under its maintenance program are adequate to support the use of its minimum equipment list.

(3) For leased aircraft maintained and operated under a U.S. operator's continuous airworthiness maintenance program and FAA-approved minimum equipment list, the foreign operator submits the U.S. operator's approved continuous airworthiness maintenance program and approved aircraft minimum equipment list to the FAA office prescribed in paragraph (b)(2) of this section for review and evaluation. The foreign operator must show that it is capable of operating under the lessor's approved maintenance program and that it is also capable of meeting the maintenance and operational requirements specified in the lessor's approved minimum equipment list.

(4) The FAA letter of authorization permitting the operator to use an approved minimum equipment list is carried aboard the aircraft. The minimum equipment list and the letter of authorization constitute a supplemental type certificate for the aircraft.

(5) The approved minimum equipment list provides for the operation of the aircraft with certain instruments and equipment in an inoperable condition.

(6) The aircraft records available to the pilot must include an entry describing the inoperable instruments and equipment.

(7) The aircraft is operated under all applicable conditions and limitations contained in the minimum equipment list and the letter authorizing the use of the list.

Docket No. 24856 (52 FR 20029) Eff. 5/28/87; (Amdt. 129–14, Eff. 8/25/87); (Amdt. 129–15, Eff. 2/25/88)

§ 129.15 Flight crewmember certificates.

No person may act as a flight crewmember unless he holds a current certificate or license issued or validated by the country in which that aircraft is with such radio equipment as is necessary to properly use the air navigation facilities, and to maintain communications with ground stations, along or adjacent to their routes in the United States.

(b) Whenever VOR navigational equipment is required by paragraph (a) of this section, at least one distance measuring equipment unit (DME), capable of receiving and indicating distance information from the VORTAC facilities to be used, must be installed on each airplane when operated between at or above 24,000 feet MSL within the 50 states, and the District of Columbia.

(Amdt. 129–2, Eff. 9/21/65); (Amdt. 129–4, Eff. 7/1/66); (Amdt. 129–7, Eff. 11/26/76)

§ 129.18 Traffic Alert and Collision Avoidance System.

(a) After December 30, 1993, no foreign air carrier may operate in the United States a turbine powered airplane that has a maximum passenger seating configuration, excluding any pilot seat, of more than 30 seats unless it is equipped with—

(1) a TCAS II traffic alert and collision avoidance system capable of coordinating with TCAS units that meet the specifications of TSO C–119, and

(2) the appropriate class of Mode S transponder.

(b) [Unless otherwise authorized by the Administrator, after December 31, 1995, no foreign air carrier may operate in the United States a turbine powered airplane that has a passenger seat configuration, excluding any pilot seat, of 10 to 30 seats unless it is equipped with an approved traffic alert and collision avoidance system. If a TCAS II system is installed, it must be capable of coordinating with TCAS units that meet TSO C–119.]

Docket No. 25355 (54 FR 951) 1/10/89; (Amdt. 129–17, Eff. 2/9/89); (Amdt. 129–21, Eff. 5/9/90); [(Amdt. 129–24, Eff. 12/29/94)]

§ 129.19 Air traffic rules and procedures.

(a) Each pilot must be familiar with the applicable rules, the navigational and communica-

(c) Each foreign air carrier shall conform to the practices, procedures, and other requirements prescribed by the Administrator for U.S. air carriers for the areas to be operated in.

§ 129.21 Control of traffic.

(a) Subject to applicable immigration laws and regulations, each foreign air carrier shall furnish the ground personnel necessary to provide for two-way voice communication between its aircraft and ground stations, at places where the Administrator finds that voice communication is necessary and that communications cannot be maintained in a language with which ground station operators are familiar.

(b) Each person furnished by a foreign air carrier under paragraph (a) of this section must be able to speak both English and the language necessary to maintain communications with the aircraft concerned, and shall assist ground personnel in directing traffic.

§ 129.23 Transport category cargo service airplanes: Increased zero fuel and landing weights.

(a) Notwithstanding the applicable structural provisions of the transport category airworthiness regulations, but subject to paragraphs (b) through (g) of this section, a foreign air carrier may operate (for cargo service only) any of the following transport category airplanes (certificated under part 4b of the Civil Air Regulations effective before March 13, 1956) at increased zero fuel and landing weights—

(1) DC–6A, DC–6B, DC–7B, DC–7C; and

(2) L–1049 B, C, D, E, F, G, and H, and the L–1649A when modified in accordance with supplemental type certificate SA 4–1402.

(b) The zero fuel weight (maximum weight of the airplane with no disposable fuel and oil) and the structural landing weight may be increased beyond the maximum approved in full compliance with applicable rules only if the Administrator finds that—

(c) No zero fuel weight may be increased by more than five percent, and the increase in the structural landing weight may not exceed the amount, in pounds, of the increase in zero fuel weight.

(d) Each airplane must be inspected in accordance with the approved special inspection procedures, for operations at increased weights, established and issued by the manufacturer of the type of airplane.

(e) A foreign air carrier may not operate an airplane under this section unless the country of registry requires the airplane to be operated in accordance with the passenger-carrying transport category performance operating limitations in part 121 or the equivalent.

(f) The Airplane Flight Manual for each airplane operated under this section must be appropriately revised to include the operating limitations and information needed for operation at the increased weights.

(g) Each airplane operated at an increased weight under this section must, before it is used in passenger service, be inspected under the special inspection procedures for return to passenger service established and issued by the manufacturer and approved by the Administrator.

(Amdt. 129–1, Eff. 4/1/65)

§ 129.25 Airplane security.

(a) The following are definitions of terms used in this section:

(1) ''Approved security program'' means a security program required by part 108 of this title approved by the Administrator.

(2) ''Certificate holder'' means a person holding an FAA air carrier operating certificate or operating certificate when that person engages in scheduled passenger or public charter operations, or both.

(3) ''Passenger seating configuration'' means the total number of seats for which the aircraft is type certificated that can be made available for passenger use aboard a flight and includes

ments conducted under contract with the Government of the United States or the Government of a foreign country; or

(ii) Passengers invited by the charterer, the cost of which is borne entirely by the charterer and not directly or indirectly by the individual passengers.

(5) "Public charter" means any charter that is not a "private charter."

(6) "Scheduled passenger operations" means holding out to the public of air transportation service for passengers from identified air terminals at a set time announced by timetable or schedule published in a newspaper, magazine, or other advertising medium.

(7) "Sterile area" means an area to which access is controlled by the inspection of persons and property in accordance with an approved security program or a security program used in accordance with § 129.25.

(b) Each foreign air carrier landing or taking off in the United States shall adopt and use a security program, for each scheduled and public charter passenger operation, that meets the requirements of—

(1) Paragraph (c) of this section for each operation with an airplane having a passenger seating configuration of more than 60 seats;

(2) Paragraph (c) of this section for each operation that will provide deplaned passengers access, that is not controlled by a certificate holder using an approved security program or a foreign air carrier using a security program required by this section, to a sterile area;

(3) Paragraph (c) of this section for each operation with an airplane having a passenger seating configuration of more than 30 seats but less than 61 seats for which the FAA has notified the foreign air carrier that a threat exists; and

(4) Paragraph (d) of this section for each operation with an airplane having a passenger seating configuration of more than 30 seats but less than 61 seats, when the Director of Civil Aviation Security or a designate of the Director has not notified the foreign air carrier in writing that a threat exists with respect to that operation.

screening by weapon-detecting procedures or facilities;

(2) Prohibit unauthorized access to airplanes.

(3) Ensure that baggage is accepted by a responsible agent of the foreign air carrier; and

(4) Prevent cargo and checked baggage from being loaded aboard its airplanes unless handled in accordance with the foreign air carrier's security procedures.

(d) Each security program required by paragraph (b)(4) of this section shall include the procedures used to comply with the applicable requirements of paragraphs (h)(2) and (i) of this section regarding law enforcement officers.

(e) Each foreign air carrier required to adopt and use a security program pursuant to paragraph (b) of this section shall have a security program acceptable to the Administrator. A foreign air carrier's security program is acceptable only if the Administrator finds that the security program provides passengers a level of protection similar to the level of protection provided by U.S. air carriers serving the same airport. Foreign air carriers shall employ procedures equivalent to those required of U.S. air carriers serving the same airport if the Administrator determines that such procedures are necessary to provide passengers a similar level of protection. The following procedures apply for acceptance of a security program by the Administrator:

(1) Unless otherwise authorized by the Administrator, each foreign air carrier required to have a security program by paragraph (b) of this section shall submit its program to the Administrator at least 90 days before the intended date of passenger operations. The proposed security program must be in English unless the Administrator requests that the proposed program be submitted in the official language of the foreign air carrier's country. The Administrator will notify the foreign air carrier of the security program's acceptability, or the need to modify the proposed security program for it to be acceptable under this part, within 30 days after receiving the proposed security program. The foreign air carrier may petition the Administrator to reconsider the notice to modify the security pro-

the following procedures apply:

(i) The Administrator notifies the foreign air carrier, in writing, of a proposed amendment, fixing a period of not less than 45 days within which the foreign air carrier may submit written information, views, and arguments on the proposed amendment.

(ii) At the end of the comment period, after considering all relevant material, the Administrator notifies the foreign air carrier of any amendment to be adopted and the effective date, or rescinds the notice of proposed amendment. The foreign air carrier may petition the Administrator to reconsider the amendment, in which case the effective date of the amendment is stayed until the Administrator reconsiders the matter.

(3) If the Administrator finds that there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes the procedures in paragraph (e)(2) of this section impractical or contrary to the public interest, the Administrator may issue an amendment to the foreign air carrier security program, effective without stay on the date the foreign air carrier receives notice of it. In such a case, the Administrator incorporates in the notice of amendment the finding and a brief statement of the reasons for the amendment.

(4) A foreign air carrier may submit a request to the Administrator to amend its security program. The requested amendment must be filed with the Administrator at least 45 days before the date the foreign carrier proposes that the amendment would become effective, unless a shorter period is allowed by the Administrator. Within 30 days after receiving the requested amendment, the Administrator will notify the foreign air carrier whether the amendment is acceptable. The foreign air carrier may petition the Administrator to reconsider a notice of unacceptability of the requested amendment within 45 days after receiving notice of unacceptability.

(5) Each foreign air carrier required to use a security program by paragraph (b) of this section are taken.

(1) If the airplane is on the ground when a bomb threat is received and the next scheduled flight of the threatened airplane is to or from a place in the United States, the foreign air carrier ensures that the pilot in command is advised to submit the airplane immediately for a security inspection and an inspection of the airplane is conducted before the next flight.

(2) If the airplane is in flight to a place in the United States when a bomb threat is received, the foreign air carrier ensures that the pilot in command is advised immediately to take the emergency action necessary under the circumstances and a security inspection of the airplane is conducted immediately after the next landing.

(3) If information is received of a bomb or air piracy threat against an airplane engaged in an operation specified in paragraph (f)(1) or (f)(2) of this section, the foreign air carrier ensures that notification of the threat is given to the appropriate authorities of the State in whose territory the airplane is located or, if in flight, the appropriate authorities of the State in whose territory the airplane is to land.

(g) Each foreign air carrier conducting an operation for which a security program is required by paragraph (b)(1), (2), or (3) of this section shall refuse to transport—

(1) Any person who does not consent to a search of his or her person in accordance with the security program; and

(2) Any property of any person who does not consent to a search or inspection of that property in accordance with the security program.

(h) At airports within the United States not governed by part 107 of this chapter, each foreign air carrier engaging in public charter passenger operations shall—

(1) When using a screening system required by paragraph (b) of this section, provide for law enforcement officers meeting the qualifications and standards, and in the number and manner, specified in part 107; and

to procedures for obtaining law enforcement assistance at that airport.

(i) At airports governed by part 107 of this chapter, each foreign air carrier engaging in scheduled operations or public charter passenger operations when using an airplane with a passenger seating configuration of more than 30 but less than 61 seats for which a screening system is not required by paragraph (b) of this section shall arrange for law enforcement officers meeting the qualifications and standards specified in part 107 to be available to respond to an incident and provide to appropriate employees, including crewmembers, current information with respect to procedures for obtaining law enforcement assistance at that airport.

(j) Unless otherwise authorized by the Administrator, each foreign air carrier required to conduct screening under this part shall use procedures, facilities, and equipment for detecting explosives, incendiaries, and deadly or dangerous weapons to inspect each person entering a sterile area at each preboarding screening checkpoint in the United States for which it is responsible, and to inspect all accessible property under that person's control.

(Amdt. 129–5, Eff. 10/9/75); (Amdt. 129–6, Eff. 8/23/76); (Amdt. 129–9, Eff. 7/25/78); (Amdt. 129–11, Eff. 9/11/81); (Amdt. 129–16, Eff. 12/21/87); (Amdt. 129–18, Eff. 4/17/89); (Amdt. 129–22, Eff. 7/31/91)

§ 129.26 Use of X-ray systems.

(a) No foreign air carrier may use an x-ray system in the United States to inspect carry-on and checked articles unless:

(1) For a system manufactured prior to April 25, 1974, it meets either the guidelines issued by the Food and Drug Administration (FDA), Department of Health, Education, and Welfare and published in the *Federal Register* (38 FR 21442, August 8, 1973); or the performance standards for cabinet x-ray systems designed primarily for the inspection of carry-on baggage issued by the FDA and published in 21 CFR 1020.40 (39 FR 12985, April 10, 1974);

efficient use of x-ray systems, and the identification of weapons and other dangerous articles;

(4) Procedures have been established to ensure that each operator of the system will be provided with an individual personnel dosimeter (such as a film badge or thermoluminescent dosimeter). Each dosimeter used will be evaluated at the end of each calendar month, and records of operator duty time and the results of dosimeter evaluations will be maintained by the foreign air carrier; and

(5) The system meets the imaging requirements set forth in an accepted Foreign Air Carrier Security Program using the step wedge specified in American Society for Testing and Materials Standard F792–82.

(b) No foreign air carrier may use an x-ray system as specified in paragraph (a) of this section—

(1) Unless within the preceding 12 calendar months a radiation survey has been conducted which shows that the system meets the applicable performance standards in 21 CFR 1020.40 or guidelines published by the Food and Drug Administration in the *Federal Register* of August 8, 1973 (38 FR 21442);

(2) After the system is initially installed or after it has been moved from one location to another, unless a radiation survey is conducted which shows that the system meets the applicable performance standards in 21 CFR 1020.40 or guidelines published by the Food and Drug Administration in the *Federal Register* on August 8, 1973 (38 FR 21442); except that a radiation survey is not required for an x-ray system that is moved to another location, if the foreign air carrier shows that the system is so designed that it can be moved without altering its performance;

(3) That is not in full compliance with any defect notice or modification order issued for that system by the Food and Drug Administration, Department of Health, Education, and Welfare, unless that Administration has advised the FAA that the defect or failure to comply is not such as to create a significant risk or injury, including genetic injury, to any person; and

photographic equipment and film packages without exposure to an x-ray system. If the x-ray system exposes any carry-on or checked articles to more than 1 milliroentgen during the inspection, the foreign air carrier shall post a sign which advises passengers to remove film of all kinds from their articles before inspection. If requested by passengers, their photographic equipment and film packages shall be inspected without exposure to an x-ray system.

(c) Each foreign air carrier shall maintain at least one copy of the results of the most recent radiation survey conducted under paragraph (b)(1) or (b)(2) of this section at the place where the x-ray system is in operation and shall make it available for inspection upon request by the Administrator.

(d) The American Society for Testing and Materials Standard F792–82, "Design and Use of Ionizing Radiation Equipment for the Detection of Items Prohibited in Controlled Access Areas," described in this section is incorporated by reference herein and made a part hereof pursuant to 5 U.S.C. 552(a)(1). All persons affected by these amendments may obtain copies of the standard from the American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103. In addition, a copy of the standard may be examined at the FAA Rules Docket, Docket No. 24115, 800 Independence Ave. SW., Washington, DC, weekdays, except Federal holidays, between 8:30 a.m. and 5 p.m.

Docket No. 15286 (41 FR 30106) 7/22/76; (Amdt. 129–6, Eff. 8/23/76); (Amdt. 129–8, Eff. 4/24/78); (Amdt. 129–10, Eff. 10/19/79); (Amdt. 129–13, Eff. 7/22/85); (Amdt. 129–23, Eff. 10/24/91)

§ 129.27 Prohibition against carriage of weapons.

(a) No person may, while on board an aircraft being operated by a foreign air carrier in the United States, carry on or about his person a deadly or dangerous weapon, either concealed or unconcealed. This paragraph does not apply to—

gage, a deadly or dangerous weapon, unless:

(1) The passenger has notified the foreign air carrier before checking the baggage that the weapon is in the baggage; and

(2) The baggage is carried in an area inaccessible to passengers.

Docket No. 15286 (41 FR 30107) 7/22/76; (Amdt. 129–5, Eff. 10/9/75); (Amdt. 129–6, Eff. 8/23/76)

§ 129.29 Prohibition against smoking.

No person may smoke and no operator shall permit smoking in the passenger cabin or lavatory during any scheduled airline flight segment in air transportation or intrastate air transportation which is—

(a) Between any two points within Puerto Rico, the United States Virgin Islands, the District of Columbia, or any State of the United States (other than Alaska or Hawaii) or between any two points in any one of the above-mentioned jurisdictions (other than Alaska or Hawaii);

(b) Within the State of Alaska or within the State of Hawaii; or

(c) Scheduled in the current Worldwide or North American Edition of the Official Airline Guide for 6 hours or less in duration and between any point listed in paragraph (a) of this section and any point in Alaska or Hawaii, or between any point in Alaska and any point in Hawaii.

(Amdt. 129–20, Eff. 2/25/90)

[§ 129.31 Airplane security.

[Each foreign air carrier required to adopt and use a security program under § 129.25(b) shall—

[(a) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need-to-know; and

[(b) Refer requests for sensitive security information by other persons to the Assistant Administrator for Civil Aviation Security.]

[(Amdt. 129–26, Eff. 4/21/97)]